University of Baltimore Law Forum

Volume 45
Number 1 *Fall 2014*

Article 3

2014

A Reasonable Expectation of Privacy Online: "Do Not Track" Legislation

Alicia Shelton
Saul Ewing LLP

ARTICLE

A REASONABLE EXPECTATION OF PRIVACY ONLINE: "DO NOT TRACK" LEGISLATION

By: Alicia Shelton[1]

INTRODUCTION

This year marked the twenty-fifth anniversary of the World Wide Web ("Web"), and more than 81% of Americans are now using the internet on a regular basis.[2] Yet, despite the fact that key pieces of personally identifying information—name, address, phone number, email address, and birthday—and sensitive personal data—political opinions, racial or ethnic origin, religious beliefs, and health—can be learned through tracking an individual's online activity, there continues to be a void of federal legislation protecting the privacy of internet users.[3] In the absence of federal action, state legislatures are tasked with regulating electronic surveillance by both private companies and the government itself, as well as establishing an expectation of privacy in the evolving digital landscape that society is prepared to recognize as reasonable.[4]

Every internet action—clicking on a website, sending an email, downloading a song, posting a photo, or instant messaging—leaves a numerical identifying mark from the computer used, allowing the user's activity to be tracked as he or she performs any online activity. Every time an individual makes an online purchase, searches for information on a personal health concern, reads a political blog, or sends an intimate message

---

[1] Associate, Saul Ewing LLP; University of Baltimore School of Law, J.D.; Davidson College, B.A.

[2] Susannah Fox & Lee Rainie, *The Web at 25 in the U.S.: The Overall Verdict: The Internet Has Been a Plus for Society and an Especially Good Thing for Individual Users*, PEW RESEARCH CTR. INTERNET PROJ., http://www.pewinternet.org/2014/02/27/the-web-at-25-in-the-u-s/ (last visited Sept. 9, 2014).

[3] Lee Rainie, et al., *Anonymity, Privacy, and Security Online*, PEW RESEARCH CTR. PROJ. (Sept. 5, 2013), http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf ; Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J. L. SCI. & TECH. 281, 349 (2012).

[4] Ganka Hadjipetrova & Hannah G. Poteat, *States Are Coming to the Fore of Privacy in the Digital Era*, 6 No. 6 LANDSLIDE 12 (July/Aug. 2014).

to a friend, that electronic action is identified by his or her Internet Protocol ("IP") address[5] and a record of the activity is captured and stored by the Internet Service Provider ("ISP").[6] Online activity can also be tracked by third-party software embedded in the web browsers used to navigate the internet.[7]

Digital privacy is federally regulated by the Electronic Communications Privacy Act (ECPA),[8] and in Maryland, it is also regulated by the Maryland Stored Communications Act (MSCA).[9] These Acts impose requirements on law enforcement officials seeking to obtain access to records or content of an individual's electronic communications stored by his or her ISP.[10] Recently, two occurrences signaled a progression in Maryland for adoption of greater

---

[5] The Sixth Circuit described the role of an IP address in identifying criminal activity as:

> [W]eb IP addresses do not directly reflect the geographic street address of the office, residence, or building from which an individual accesses his email and/or the Internet. Instead, law enforcement officials must conduct research and rely upon the addresses and data provided by internet providers, such as AOL and Insight Communications, as well as billing addresses for those service providers and/or credit card companies. Yet, the IP address assignment…is most telling in regards to which individual…used it to access the sites containing the suspect material.

United States v. Wagers, 339 F. Supp. 2d 934, 940, *aff'd* by United States v. Wagers, 452 F.3d 534 (6th Cir. 2006).

[6] Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected As Personally Identifiable Information.*, 60 DEPAUL L. REV. 895, 930-31 (Spring 2011) ("To say that Internet subscribers voluntarily exposed this information to ISPs is simplistic and misleading. After all, the only way to avoid releasing this information to an ISP is to not use the Internet at all.") (citing Daniel J. Solove, *Reconstructing Electronic Surveillance Law.*, 72 GEO. WASH. L. REV. 1264, 1287 (2004)).

[7] *See generally* Jonathan Mayer & Arvind Narayanan, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers* (Feb. 18, 2011), *available at* http://donottrack.us.docs/FTC_Privacy_Comment_Stanford.pdf.

[8] 18 U.S.C.A. § 2510, et seq.

[9] MD. CODE ANN., CTS. & JUD. PROC. § 10-4A-01 et seq.

[10] 18 U.S.C.A. §§ 2701(a)-(b) (2014); MD. CODE ANN., CTS. & JUD. PROC. § 10-4A-04 (West 2008).

regulation and enforcement in digital privacy protection: the adoption of House Bill 912,[11] amending the MSCA to expand the search warrant requirement for a law enforcement officer requesting content of electronic communications that have been in electronic storage with an ISP for any amount of time; and the creation, under Attorney General Douglas Gansler, of an Internet Privacy Unit,[12] tasked to address issues in online privacy policies.

This comment proposes that Maryland should extend the privacy protections recognized by HB 912 to further protect individuals from online tracking by third parties through imposing "Do Not Track" requirements on search engines and websites. Part One will discuss current internet technology and usage, as well as the resulting increase in privacy concerns. Part Two will discuss developments in privacy protection legislation and the growing role of state legislatures in safeguarding an individual's privacy online. Part Three will discuss other states' practices and possible additional protections which could be enacted by the Maryland Legislature, and enforced by the Maryland Internet Privacy Unit, to address growing concerns regarding internet privacy.

II. INTERNET USAGE AND GROWING PRIVACY CONCERNS

A. Prevalence of Internet Usage in the United States

In 1989, when the World Wide Web was "born,"[13] only 15% of U.S. households had a computer.[14] By 1997 only 18% of U.S. households used computers to access the internet,[15] however, by 2012 that number had risen to almost 75% of households, and this year an estimated 81% of Americans will access the internet through personal computers, smartphones, and

---

[11] H.B. 912, 2014 Leg., 431st Sess. (Md. 2014).

[12] Douglas F. Gansler: Press Release, *Attorney General Gansler Forms Internet Privacy Unit: Data Privacy Day Heightens Focus on Online Safety Efforts*, OFFICE OF THE MD. ATT'Y GEN. (Jan. 28, 2013), http://www.oag.state.md.us/Press/2013/012813.html.

[13] Fox & Rainie, *supra* note 2, at 1.

[14] *Households with a Computer and Internet Use: 1984-2009*, UNITED STATES CENSUS BUREAU, http://www.census.gov/hhes/computer/publications/ (last visited Oct. 2, 2014).

[15] "The Internet is a networking infrastructure, a network of networks that connects millions of computers together using the Internet Protocol. The World Wide Web ('Web') is an open network, information-sharing service that operates over the Internet using the HTTP ('Hypertext Transfer Protocol') format." WILLIAM F. PATRY, PATRY ON FAIR USE: COMPUTERS – INTERNET USES, 259-61 (2014) (footnotes omitted).

tablets.[16] Internet usage continues to play an increasing role in individuals' lives. More than half of all Americans go online daily to send and receive email messages[17] and of 73% of the internet population that used social media sites last year,[18] the average Facebook[19] user had 350 "friends" online. [20] In addition to using the internet as a regular mode of communication, more than a third of all Americans have searched online to research intimate personal information such as medical conditions.[21] The internet continues to rapidly expand consumer services, such as shopping, browsing and comparing products. In the last year alone, over 191.1 million U.S. citizens bought at least one item online.[22]

B. Getting Connected Online

Over the last ten years, not only has the percentage of Americans that use the internet, and the types of activities they conduct online, rapidly expanded, but now people connect to the internet in many varied ways as

---

[16] *Households with a Computer and Internet Use*, *supra* note 12, at 3; Susannah Fox & Lee Rainie, *How the Internet Has Woven Itself Into American Life*, PEW RESEARCH CTR. INTERNET PROJ., (Feb. 27, 2014), http://www.pewinternet.org/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life/.

[17] *Typical Daily Activities of Adult Internet Users in the United States as of 2012, by Age Group*, STATISTA, http://www.statista.com/statistics/184541/typical-daily-online-activities-of-adult-internet-users-in-the-us/ (last visited Oct. 2, 2014).

[18] *Share of U.S. Adult Internet Users Who Use Social Networking Sites from 2005 to 2013*, STATISTA, http://www.statista.com/statistics/273035/share-of-us-adult-internet-users-who-use-social-networking-sites/ (last visited Oct. 2, 2014).

[19] "Facebook, the behemoth of the social networking world, allows users to build a profile and interact with 'friends.'" Griffin v. State, 419 Md. 343, 354, 19 A.3d 415, 421 (2011).

[20] *Average Number of Facebook Friends of U.S. Users in 2014, by Age Group*, STATISTA, http://www.statista.com/statistics/232499/americans-who-use-social-networking-sites-several-times-per-day/ (last visited Oct. 2, 2014).

[21] Susannah Fox & Maeve Duggan, *Health Online 2013*, PEW RESEARCH CTR. INTERNET PROJ., (Jan. 15, 2013), http://www.pewinternet.org/2013/01/15/health-online-2013/.

[22] *Number of Digital Shoppers in the United States from 2010 to 2018 (in millions)*, STATISTA, http://www.statista.com/statistics/183755/number-of-us-internet-shoppers-since-2009/ (last visited Sept. 20, 2014).

well.[23] The internet, "a network of networks that connects millions of computers together," allows data such as email, documents, media, images, music, and web pages, to be transmitted between computers.[24] Within the internet, the Web "permits pages that are formatted with Hypertext Markup Language ("HTML"), as well as images, documents created with word processors, and other files to be posted for public viewing by anyone with Internet access . . . by use of a domain name system ("DNS") that assigns an IP address used by computers to identify and communicate with each other."[25]

Early internet connection was reliant on a physical cable that connected the cable jack to a modem, which then ran to one computer.[26] The advent of wireless networks and computers with internal modems eliminated the need for those hardwired connections, allowing multiple users to use one internet connection through transmission of a wireless signal.[27]

In 2001 about half of all Americans used the internet, but only approximately 4% had home wireless networks compared to 63% in 2011 that used wireless networks to go online with their laptops or phones from multiple locations beyond just home and work.[28] The broad accessibility of wireless networks means that "Internet access is no longer synonymous with going online with a desktop computer."[29] Going wireless generally requires connecting an internet "access point"—like a cable or DSL modem—to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. When an individual connects to the Internet, a sixteen digit IP address[30] identifies the wireless network connection point that the

---

[23] Kathryn Zickuhr & Aaron Smith, *Digital Differences*, PEW RESEARCH CTR. INTERNET PROJ., 1, 2-4 (Apr. 13, 2012), *available at* http://www.pewinternet.org/files/oldmedia/Files/Reports/2012/PIP_Digital_differences_041312.pdf.

[24] Patry, *supra* note 13, at 260-61.

[25] *Id.* at 261.

[26] ROUZBEH YASSINI ET AL., PLANET BROADBAND (John Kane ed. 2004), *available at* http://www.informit.com/library/content.aspx?b=Planet_Broadband&seqNum=17.

[27] *Id.*

[28] Zickuhr & Smith, *supra* note 20, at 8.

[29] *Id.* at 2.

[30] This sixteen digit numerical identifier, the Internet Protocol (IP) address, is assigned by the Internet Service Provider (ISP), such as Comcast or Verizon, which provides its customer with access to the Internet. Russ Smith, *IP Address: Your Internet Identity*, NATIONAL TELECOMMUNICATIONS & INFORMATION

computer, smart phone, tablet, or device uses, leaving behind digital footprint of all the user's internet activity.

After a user has established an internet connection, web browsers are used to navigate among sites on the Web:

> Because Web sites are collections of pages and the pages are not always a single document but instead may consist of multiple elements . . . there are different URLs within one Web site. Those different URLs are not necessarily stored on the same server as the main web page. In order to read the web page, a browser such as Mozilla or Firefox is used. The browser combines all of the elements of the Web site in order to display the page sought (whether the home page or internal pages). The browser also permits users to navigate from one page within one site to another page, and to follow links to different sites.[31]

C. Internet Monitoring and Tracking

When using the internet or navigating the Web, an individual's activity can be tracked and stored in a variety of ways. The information gathered from tracking a user's activity can offer many benefits to the user, including customizing online experiences, saving a user's preferences for future access to specific websites, or completing transactions such as purchasing products.[32] The information also allows websites to gather beneficial

---

ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, http://www.ntia.doc.gov/legacy/ntiahome/privacy/files/smith.htm (Mar. 29, 1997); *IPv6 Guide Provides Path to Secure Deployment of Next-Generation Internet Protocol*, NATIONAL INSTITUTE STANDARDS AND TECHNOLOGY, http://www.nist.gov/itl/csd/ipv6_010511.cfm (last visited Jan. 21, 2013); *Number Resources*, INTERNET ASSIGNED NUMBERS AUTHORITY, http://www.iana.org/numbers (last visited Sept. 20, 2014); The global database of IP addresses is managed by the Internet Assigned Numbers Authority and allocated in the United States by the American Registry for Internet Numbers. *See ARIN at a Glance*, AMERICAN REGISTRY FOR INTERNET NUMBERS, https://www.arin.net/about_us/overview.html (last visited Sept. 20, 2014). When an individual registers with an ISP, like Comcast or Verizon, she is assigned an IP address for the term of the contract with them. ISPs assign IP addresses through a Dynamic Host Configuration Protocol server, and while they don't change often for a registered user, under specific circumstances the ISP will release and/or renew the IP address. When the service contract ends, the numerical identifier that is the IP address will be recycled by the ISP and assigned to a new customer. *Release and renew your IP address*, COMCAST, http://customer.comcast.com/help-and-support/internet/releasing-and-renewing-ip-address/ (last updated Apr. 8, 2014).

[31] Patry, *supra* note 13, at 262.

[32] *See generally* Tene & Polonetsky, *supra*, note 3, at 1.

analytics, such as visitor traffic volume, areas of origin of website visitors, and tracking the effectiveness of advertisements on the website.[33] Yet, there is a dearth of sensitive personal information that can be revealed through tracking website access by individual users, such as health conditions, financial status, political opinions, religious beliefs, racial or ethnic backgrounds, and intimate relationships, with users having no control over how, or to whom, the information is transmitted.[34]

Internet activity tracking is used frequently by online advertising networks to create target advertisements based on users' individual preferences by tracking the user in a variety of ways. To target ads to those users, those third party ad networks also try to collect every iota of information they can about site visitors — the idea is that the more in tune [] an ad is with a user's interests and tastes, the more likely they are to click. Usually, targeting starts off with the same sort of general details in HTTP headers — browser, IP address, etc. However, each of these third party ad networks will also try to store cookies on the browser for later reference. If that same browser later visits another site serviced by the same ad network, it will be recognized and the advertising service now knows "Ah, in addition to being near Arlington, Virginia, and loading pages about Web browser privacy, this browser also visits pages related to My Little Pony. How interesting." Suddenly the ad network knows not just technical details of a browser, but potentially very personal information about its user. (Don't think so? Substitute "HIV testing" or "bankruptcy attorney" for My Little Pony, above.) Suddenly, ads served to that browser by that ad company may take on a very different character.[35]

The use of "cookies" carries information between web pages, allowing a site to re-identify visitors and storing individual information, such as log-in credentials, name, email address and more.[36] Cookies can be specific to one domain or Uniform Resource Locator ("URL"), or can be stored on a user's computer as a small text file placed by a third party, such as an advertising network, to allow tracking of the internet user as he or she moves across many websites.[37] Cookies can be managed by internet users, but few

---

[33] *Id.*

[34] *See generally What They Know*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Sept. 15, 2014).

[35] Geoff Duncan, *Why Do Not Track May Not Protect Anybody's Privacy*, DIGITAL TRENDS (June 9, 2012), http://www.digitaltrends.com/mobile/why-do-not-track-may-not-protect-anybodys-privacy/#ixzz3CMDT9hMu.

[36] Microsoft Support, *Description of Cookies*, MICROSOFT, http://support.microsoft.com/kb/260971 (last visited Sept. 8, 2014).

[37] *Id.*

understand how to manage the settings and some websites are no longer accessible if the user has elected to block cookies.[38]

A user's internet activity can also be tracked by "browser fingerprinting" through which:

> [S]eemingly innocuous bits of information, such as a browser's version number, plugins, operating system, and language, websites can uniquely identify ("fingerprint") a browser and, by proxy, its user. Not only do browser fingerprints track users more accurately than cookies, they are also harder to detect and control . . . [f]ingerprinting is largely invisible, tough to fend off and semi-permanent."[39]

Additionally, mobile devices can be tracked not only through activity on web browsers, but also through downloaded "apps" to transmit the device's unique device identifier to third parties to reveal internet activity, the user's name, phone number, and physical location.[40]

A 2012 report found that the top one hundred most popular websites all tracked users' online activity, recording web browser searches and subsequently visited websites, to target advertisements.[41] Is it therefore generally accepted by society that all individuals should know that all online activity is stored, tracked, and potentially sold to advertisers? With increasing information on how private emails can be accessed and searched, and how even information that individuals assume to be private can be collected and stored by ISPs, is it reasonable to have any expectation of privacy online?[42] The question remains as to what we should expect most

---

[38] Tene & Polonetsky, *supra*, note 3, at 292.

[39] *Id*. at 294-95 (internal citation omitted).

[40] *Id.* at 296. "An examination of 101 popular smartphone 'apps'—games and other software applications for iPhone and Android phones—showed that [fifty-six] transmitted the phone's unique device ID to other companies without users' awareness or consent. Forty-seven apps transmitted the phone's location in some way. Five sent age, gender and other personal details to outsiders." Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J., (Dec. 18, 2010), http://online.wsj.com/news/articles/SB10001424052748704368004576027751867039730.

[41] Andrew Couts, *Top 100 Websites: How They Track Your Every Move Online*, DIGITAL TRENDS (Aug. 30, 2012), http://www.digitaltrends.com/web/top-100-websites-how-are-they-tracking-you/.

[42] *Fact Sheet 18: Online Privacy: Using the Internet Safely*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/fs/fs18-cyb.htm#PART_ONE (last updated July 2014).

individuals, or "society" to know about the information they communicate on the internet, and whether society would expect an individual to know the full extent of how personal information is tracked, stored, and distributed by third parties and ISPs, as well as the retention and availability of personal information even after an individual "deletes" it.[43]

D. Societal Concerns over Internet Monitoring and Tracking

As internet users continue to rely more heavily on the internet to conduct private activities on a regular basis, concerns for privacy have grown as well. "The major effect of the computer on privacy is that computers prevent the individual from deciding whether that information will be released. This loss of control can be either loss of access control or loss of accuracy control."[44] In phone interviews conducted of 1,480 adults in the U.S. in 2013 regarding internet tracking and information gathering by the government, "a majority of Americans—56%—say that federal courts fail to provide adequate limits on the telephone and internet data the government is collecting as part of its anti-terrorism efforts. An even larger percentage (70%) believes that the government uses this data for purposes other than investigating terrorism."[45] When asked about their concerns with government monitoring of internet data, almost half expressed that they felt the government had "gone too far in restricting the average person's civil liberties[,]" which was a fifteen point rise from when the same question asked three years earlier.[46]

Concerns over internet use monitoring by third parties exceeds the concerns regarding governmental activity. In a recent survey by the Pew Research Center of 1,802 internet users,[47] more than 86% had "taken steps to remove or mask their digital footprints—ranging from clearing cookies to

---

[43] *See generally Data on the Internet is Permanent After 20 Minutes*, INFOSECURITY MAG. (Apr. 21, 2011), http://www.infosecurity-magazine.com/view/17536/data-on-the-internet-is-permanent-after-20-minutes/ (information posted on the Internet becomes permanent after twenty minutes, so that it is stored and retained even if the user thinks that he or she has deleted it).

[44] 1 VIRGINIA V. SHUE & JAMES V. VERGARI, STATE COMPUTER LAW: COMMENTARY, CASES & STATUTES § 4:1 (Thomson Reuters) (Aug. 2014).

[45] Michael Dimock & Caroll Doherty, *Few See Adequate Limits on NSA Surveillance Program*, PEW RESEARCH CTR. (July 26, 2013), *available at* http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf.

[46] *Id.*

[47] Rainie, et al., *supra*, note 3, at 1. For purposes of the survey, an "internet user" was defined as "someone who uses the internet, sends/receives email, or accesses the internet [on] a mobile device." *Id.*

encrypting their email, from avoiding using their name to using virtual networks that mask their Internet Protocol (IP) address."[48] Yet, more than 20% said they had their email or social networking accounts hacked or taken over, and 11% said they had crucial personal information such as their social security numbers, credit cards, or bank accounts stolen.[49]

E. Societal Expectations on Legislation to Protect Privacy

In the Pew Research Center's 2013 report, when asked whether internet users felt current legislation was sufficient to protect their online privacy, 68% of the internet users surveyed expressed that they "believe current laws are not good enough in protecting people's privacy online[,]" and 50% also expressed that they were "worried about the amount of personal information about them that is online—a figure that has jumped from 33% who expressed such a worry in 2009."[50] Concern for online privacy is not just in the content of emails and communications, but a majority expressed that they felt it was "very important" that they could keep private the records of their internet activity, such as the identity of who they communicate with, what they download, and where they access the internet—all of which is identifiable by an IP address.[51]

In an online survey by Zogby International[52] of 2,111 U.S. adults, 87% expressed concern over the safety of their personal information online and 80% were concerned that their online habits were being recorded by third parties to generate a profit in advertising.[53] In response, 88% felt that consumers online should enjoy similar legal privacy protections as their "off-line" counterparts, and half of all surveyed wanted the government to play a larger role in protecting their online privacy.[54]

---

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] Zogby Int'l, *Results From June 4-7 Nationwide Poll*, 1 (June 7, 2010), *available at* http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf ("A sampling of Zogby International's online panel, which is representative of the adult population of the U.S., was invited to participate.").

[53] *Id.*

[54] *Id.*

III: DEVELOPMENTS IN PRIVACY PROTECTION LAWS AND THE ROLE OF STATE LEGISLATURES

A. Historical Principles and Development of Privacy Protection Laws as it Effects Digital Privacy Regulation

Historically, legal protections enacted to safeguard individual privacy are rooted in Fourth Amendment[55] principles, which restrict searches and seizures by the government to safeguard individual privacy. For the Fourth Amendment to apply, an individual must have a reasonable expectation of privacy in the place to be searched or the thing to be seized, incorporating both an individual's subjective expectation of privacy and also the conclusion that the expectation is one that society would recognize as objectively reasonable.[56] In *Katz v. United States*, the Supreme Court noted that "the Fourth Amendment protects people not places" and what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[57] In *Raynor v. State*, the Court of Appeals of Maryland explained the relationship between individual and societal expectations of privacy:

> A person demonstrates a subjective expectation of privacy by showing that he or she sought "to preserve something as private." . . . An objectively reasonable expectation of privacy, by contrast, has "'a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society,' and constitutes more than a subjective expectation of not being discovered." . . . We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable . . . . Nonetheless, common experience and social norms bear upon our assessment of whether one has an objectively reasonable expectation of privacy in a particular item or place . . . . Expectations of privacy are established by general social norms . . . . [I]t is necessary to look to the customs and values of the past and present, the structure of society, the patterns of interaction, [and] the web of norms and values.[58]

---

[55] U.S. CONST. amend. IV ("No Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.").

[56] United States v. Jacobsen, 466 U.S. 109, 113 (1984); California v. Greenwood, 486 U.S. 35, 39-40 (1988).

[57] Katz v. United States, 389 U.S. 347, 351, 88 S. Ct. 507, 511 (1967).

[58] Raynor v. State, No. 69, 2014 WL 4216019, at *6 (Md. Aug. 27, 2014) (internal quotations and citations omitted) (alterations in original).

Common expectations of privacy must necessarily change as society technologically advances. In determining an objective expectation of privacy, courts also look to "widely shared social expectations."[59] In 2001, in *Kyllo v. United States*, the Supreme Court explored "what limits there are upon this power of technology to shrink the realm of guaranteed privacy[,]" noting that advances in technology have eroded the degree of privacy secured to individuals.[60]

Ten years later, in *United States v. Jones*, the Supreme Court again addressed the effect of technological advances in electronic surveillance on societal expectations of privacy.[61] Justice Sotomayor's concurrence describes the amount of invasive information gathered from GPS monitoring, information similar to what can be gleaned from tracking someone's online activity—"a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations" that could be stored "and efficiently mine[d] . . . for information years into the future" in a manner which "is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks."[62]

As Justice Alito expressed in her concurrence in *Jones*, shared social expectations are difficult to define in the courts because, not only must they necessarily change as society advances, they are subject to the individual interpretation of the court that is defining them:[63]

The basic problem is that the inner workings of the Internet and other digital technologies produce a much larger data trail than most people expect, and portions of that data trail are available to more people and companies than most would expect. And because judges base society's expectations on the nature of the underlying technology, the gap persists and increases as technology progresses.[64]

B. The Federal Electronic Communications Privacy Act of 1986

---

[59] Georgia v. Randolph, 547 U.S. 103, 129, 126 S. Ct. 1515, 1531 (2006).

[60] Kyllo v. United States, 533 U.S. 27, 33-34, 121 S. Ct. 2038, 2043 (2001).

[61] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[62] *Id.* at 955-56.

[63] *Jones*, 132 S. Ct. at 962-64.

[64] Brandon T. Crowther, *(Un)Reasonable Expectation of Digital Privacy*, 2012 BYU L. REV. 343, 351-52 (2012) (footnotes omitted).

The Federal Electronic Communications Privacy Act of 1986 ("ECPA")[65] regulates under which circumstances a telecommunication or ISP can disclose information to third parties. Currently, federal legislation restricts government access to electronic communications through the ECPA in three ways: Title I regulates accessing electronic communications in transmission under its wire-tap provisions;[66] Title II restricts access to stored electronic communications, the Stored Communications Act ("SCA");[67] and Title III regulates the tracing of electronic communications by the "pen register/trap"[68] provisions. There have been only limited amendments to the ECPA since its inception, none of which provided any additional privacy protections to internet users nor extended to tracking by private parties, despite growing concerns over the vast amount of personal information which can now be gleaned from one's internet use.[69]

The ECPA regulates instances in which ISPs can disclose subscriber identification information, stored communications, and other maintained information to the government or private individuals, as well as what is required for disclosure.[70] The ECPA was intended to balance law enforcement needs with personal privacy concerns in the newly emerging internet landscape:[71]

> [It] reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in the content of stored

---

[65] 18 U.S.C. §§ 2701-2705 (2012).

[66] 18 U.S.C. §§ 2510-2522 (2012).

[67] 18 U.S.C. §§ 2701-2705 (2012).

[68] 18 U.S.C. §§ 3121-3127 (2012).

[69] 47 U.S.C. §§ 1001-1010 (In 1994, the ECPA was first amended by the Communications Assistance for Law Enforcement Act); Pub. L. No. 107-56, 115 Stat. 272 (In 2001 and 2006, it was further amended by the USA PATRIOT Act and its reauthorization act); Pub. L. No. 110-261, 122 Stat. 2436 (Most recently, it was amended by the FISA Amendments Acts of 2008); *see* https://it.ojp.gov/default.aspx?area+privacy&page=1285.

[70] Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191, 215 (2011).

[71] J. Beckwith Burr, *The Electronic Communications Privacy Act of 1986: Principles for Reform*, COALITION (2010), *available at* http://digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

> emails than in subscriber account information. Similarly, the drafters believed that computing services available "to the public" required more strict regulation than services not available to the public.[72]

The ECPA has been interpreted in federal courts to provide that there is not an expectation of privacy in information that was voluntarily given to a third party, and in the event that the information was improperly disclosed, the ECPA allowed for only civil remedies, not suppression.[73] In 2001, the ECPA was interpreted to have repealed the provisions of the Cable Communications Privacy Act that required notification of customers when their information was disclosed.[74] Under the ECPA, ISPs can be forced to disclose subscribers' information and are prevented from notifying the subscriber in several instances.[75] The ECPA has been interpreted to support that "individuals have no Fourth Amendment privacy interest in subscriber information given to ISP[s]."[76]

In 2011 Senator Leahy, the original sponsor of the ECPA, proposed its amendment to account for the changes in how the internet is used. He noted that:

> Since the Electronic Communications Privacy Act was first enacted in 1986, ECPA has been one of our nation's premiere privacy laws…[b]ut, today, this law is significantly outdated and out-paced by rapid changes in technology and the changing mission of our law enforcement agencies after September 11. Updating this law to reflect the realities of our time is essential to ensuring that our federal privacy laws keep pace with new technologies and the new threats to our security.[77]

---

[72] OFFICE OF LEGAL EDUCATION EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS, UNITED STATES DEPT. OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, at 115-16 (2009).

[73] United States v. Hambrick, 55 F. Supp. 2d 504, 507, 509 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000).

[74] *In re Application* of U.S. for an Order Pursuant to 18 U.S.C. §2703(d) Directed to Cablevision Sys. Corp., 158 F. Supp. 2d 644, 648-49 (D. Md. 2001).

[75] 18 U.S.C. § 2705(b)(1)-(5) (2012).

[76] United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005).

[77] Senator Patrick Leahy, *Leahy Introduces Benchmark Bill To Update Key Digital Privacy Law*, WEBSITE OF PATRICK LEAHY, UNITED STATES SENATOR FOR

C. State vs. Federal Regulation of Digital Privacy

Justice Alito's concurrence in *Jones* suggests that the proper body to establish protection of individuals' privacy amidst electronic surveillance is the Legislature because the "legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[78]

Post-*Jones*, Congress has yet to enact legislation providing additional privacy safeguards to keep up with technological advancements, but several authors suggest that state legislatures might be in a better position to enact privacy safeguards, especially in regard to technological advancements, due to efficiency in enacting legislation at the state level in the rapidly advancing field—state lawmakers are in a better position to evaluate their constituents attitudes and societal expectations, and "state legislation conveys information about societal values . . . ."[79]

In absence of increased federal regulation, "in the last two decades, more than two-thirds of states have either passed or considered privacy laws in the internet and social media context."[80] Additionally, although the Federal Trade Commission has historically been the "primary federal enforcement agency in the sphere of privacy and data security," states are taking an increasing role in digital privacy regulation and enforcement, due to the lack of comprehensive federal privacy law.[81]

D. The Maryland Stored Wire and Electronic Communications and Transactional Records Access Act

Two years after the ECPA was originally enacted, in 1988, Maryland adopted the Stored Wire and Electronic Communications and Transactional

---

VERMONT, PRESIDENT PRO-TEMPORE OF THE UNITED STATES SENATE (May 17, 2011), http://www.leahy.senate.gov/press/leahy-introduces-benchmark-bill-to-update-key-digital-privacy-law (last visited Oct. 2, 2014).

[78] United States v. Jones, 132 S. Ct. 945, 964 (2012).

[79] Colin Shaff, *Is the Court Allergic to Katz? Problems Posed by New Methods of Electronic Surveillance to the "Reasonable-Expectation-of-Privacy" Test*, 23 S. CAL. INTERDISC. L.J. 409, 410, 440 (2014); Henry F. Fradella et. al., *Quantifying Katz: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 337-39 (2011).

[80] Hadjipetrova & Poteat, *supra*, note 4 at 14.

[81] *Id.* at 13.

Records Access Act ("SCA").[82] The Maryland SCA originally mirrored the ECPA but it did not provide the exigent circumstances disclosure provision that the federal statute allowed.[83] In 2008, the Maryland legislature passed the Maryland Personal Information Act, providing that businesses are statutorily mandated to protect the security of personal information of individuals.[84] However, it failed to address personal information maintained on the Internet, limiting its coverage to specific data.[85]

Maryland criminalizes the unauthorized access of computers and related material, suggesting that in the future, when determining how to address privacy in wireless networks, there might be an expectation of privacy when the network is secured or password protected.[86] Even though it did not specify information maintained in electronic databases or on the web, this law, in conjunction with the Maryland Personal Information Protection Act, signals that Maryland recognizes the necessity of protecting its citizen's personal information that has become ever increasingly accessible.

In 2007, the Court of Appeals of Maryland had its "first opportunit[y] to consider legal issues arising from an Internet communications context," [87] defining the internet as "a global network of computers, [where] 'each computer connected to the Internet must have a unique address'[88] known as an Internet Protocol Address, which 'can be used to identify the source of the

---

[82] MD. CODE ANN., CTS. & JUD. PROC. § 10-4A-01 (West 1988).

[83] Upshur v. State, 208 Md. App. 388, 393, 56 A.3d 620, 624-25 (2012).

[84] MD. CODE ANN., COM. LAW § 14-3503.

[85] MD. CODE ANN., COM. LAW § 14-3503; *see also Maryland Personal Information Protection Act*, BUS. & TECH. LAW GRP., http://www.btlg.us/News_and_Press/articles/Personal%20Information%20Protection%20Act (last visited Oct. 2, 2014).

[86] MD. CODE ANN., CRIM. LAW § 7-302 (West 2012); Briggs v. State, 348 Md. 470, 481, 483, 704 A.2d 904, 910, 911 (1998) ("Intent of the General Assembly was to criminalize the misuse of computers or computer networks by those whose initial access was unauthorized … These comments and reports suggest that the intent of the Legislature was to punish access that was not initially authorized and not to punish conduct that merely exceeded authorized access.").

[87] Independent Newspapers, Inc. v. Brodie, 407 Md. 415, 419-20, 966 A.2d 432, 435 (2009) (citing Beyond Sys., Inc. v. Realtime Gaming Holding Co., 388 Md. 1, 20-21, 878 A.2d 567, 589 (2005)).

[88] *Beyond Sys.*, 388 Md. at 21, 878 A.2d at 579 (citing Rus Shuler, How Does the Internet Work? THESHULERS.COM http://www.theshulers.com/whitepapers/internet_whitepaper/ (last visited Oct. 2, 2014)).

connection' to the Internet . . . [that] is then transmitted via an Internet Service Provider."[89]

In 2009, the Court of Appeals of Maryland began to address the issue in the context of internet defamation.[90] The court of appeals noted that as communication opportunities continue to develop on the Internet, the court will continue to be presented with new issues.[91] The court reasserted the Internet definition provided in *Beyond Systems, Inc. v. Realtime Gaming Holding Co.*, and expanded its discussion to email transmissions, instant messaging, internet chat rooms, and anonymity on the internet.[92]

In *Upshur v. State*, the Court of Special Appeals of Maryland held that under the EPCA and Maryland SCA, the defendant had no reasonable expectation of privacy in information provided to his mobile service provider, and that neither statutory provision provided a suppression remedy even if the information had been unlawfully obtained.[93]

Recently, the adoption of House Bill 912,[94] amending the Maryland SCA, marked a recognition by the Maryland legislature of an increased need for privacy protections of an individual's online communications. House Bill 912 amended the Maryland SCA to require law enforcement officers to obtain a search warrant, supported by probable cause, in order to request the content of electronic communications in electronic storage for any amount of time, and also extended the search warrant requirement to stored "records or other information" sought without notice to the subscriber.[95]

Within the last few years, Maryland has enacted additional digital privacy legislation, such as data breach notification laws in the Maryland Personal

---

[89] *Beyond Sys.*, 388 Md. at 21, 878 A.2d at 579 (citing United States v. Bach, 400 F.3d 622, 625 n.4 (8th Cir. 2005)).

[90] *Independent Newspapers, Inc.*, 407 Md. at 421-22, 966 A.2d at 436.

[91] *Id.*

[92] *Id.* at 421-26, 966 A.2d at 436-41.

[93] Upshur v. State, 208 Md. App. 388, 386, 56 A.3d 620, 628 (2012). *See also In re § 2703(d)* Order, 787 F.Supp.2d 430, 436 (E.D. Va. 2011) (explaining that the subscribers had no protected privacy interest in their IP addresses they used, data volume transfers, the receiving source and destination IP addresses that they "tweeted" communications to, or Twitter's correspondence notes related to the individual's accounts) (citing United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010)). The Eastern District of Virginia also held that a defendant has no reasonable expectation of privacy in information that was voluntarily given to the third party ISP. *Id.*

[94] H.B. 912, 2014 Leg., 431st Sess. (Md. 2014), fiscal and policy note.

[95] *Id.*

Information Protection Act,[96] and restrictions on employers' access to their employees' social media accounts.[97]

Additionally, in 2013, in recognition of the increase in Internet crime in Maryland, the Maryland Office of the Attorney General launched the new "Internet Privacy Unit" tasked to "address the problem of privacy in the Internet age and to update 'gaps' in companies' online privacy policies."[98] Attorney General Gansler described the Unit's objectives to:

[M]onitor companies to ensure they are in compliance with state and federal consumer protection laws, . . . examine weaknesses in online privacy policies and work alongside major industry stakeholders and privacy advocates…[and] pursue enforcement actions where appropriate to ensure consumers' privacy is protected."[99]

In 2013, Attorney General Gansler successfully "led a charge by [thirty-six] state attorneys general to demand accountability from Google when it unilaterally changed its privacy policy" by collecting "information on consumers' internet browsing activity without their consent . . . [by] using the type of code that overrides users' privacy settings."[100]

IV. PROTECTIONS MARYLAND COULD ENACT TO ADDRESS GROWING CONCERNS FOR INTERNET PRIVACY

At the time the EPCA and the Maryland SCA were enacted, the internet was primarily used by government, academics, and industrial researchers, not achieving widespread public use until years later.[101] While more

---

[96] MD. CODE ANN., COM. LAW §§ 14-3502-3508.

[97] MD. CODE ANN., LAB. & EMPL. § 3-712.

[98] Kate Havard, *Maryland Attorney General Launches Internet Privacy Unit*, WASH. POST, Jan. 28, 2013, http://www.washingtonpost.com/local/md-politics/maryland-attorney-general-launches-internet-privacy-unit/2013/01/28/345509a0-697a-11e2-ada3-d86a4806d5ee_story.html (last visited Oct. 2, 2014). "In 2011, Maryland ranked seventh out of 50 states in reported incidents of Internet crime on a per capita basis, according to the FBI's Internet Crime Complaint Center." *Id.*

[99] Gansler, *supra* note 12, at 3.

[100] *Id.;* Scott Dance, *Google to Pay Md. $1M Over Privacy Breach Allegations: State Led Investigation to Reach $17M, 37-state Settlement*, THE BALT. SUN (Nov. 18, 2013), http://articles.baltimoresun.com/2013-11-18/business/bs-bz-google-privacy-settlement-20131118_1_default-privacy-privacy-preferences-privacy-settings.

[101] Laura J. Tyson, *A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover an Internet User's Identity*, 40 SETON HALL L. REV. 1257, 1284 (2010).

sophisticated users might understand the information that is conveyed, retained, stored, and possibly made accessible every time they log onto the internet, the expectation that accessing the internet sacrifices all expectation of privacy should not be one that society is willing to accept.

A. "Do Not Track" Legislation

In 2007, the Federal Trade Commission began exploring the use of a "Do Not Track" list for online advertisers.[102] In 2009, in response to the Federal Trade Commission's exploration of a Do Not Track list,[103] Christopher Soghoian, Sid Stamm, and Dan Kaminsky proposed a "technology standard intended to enable individual Web users to express whether or not they consent to having their online activities monitored and collated, mostly for the purpose of being served targeted advertising."[104] As originally proposed, Do Not Track was not regulated by a federal or state body, but was purely a voluntary effort from the technology community.[105] The Do Not Track operates to:

> At a very basic level, Do Not Track is elegantly simple. If Do Not Track is active, a user's Web browser sends a single HTTP header to remote servers along with every request for pages, images, and any other constituent items that make up a Web page. Whenever you load a Web page, your browser sends a flurry of headers to the remote system indicating not just the specific page you want, but what types of media you can handle, your preferred languages, any cookies the site had previously set for you, information about your Web browser, and more.
>
> The Do Not Track header is called, logically, enough, DNT. If the value of that header is "1," the header serves as a signal to the server that the user does *not* wish to be

---

[102] Jasmin Melvin, "*Do Not Track" Internet Spat Risks Legislative Crackdown*, REUTERS (July 23, 2012), http://www.reuters.com/article/2012/07/23/us-internet-tracking-idUSBRE86M17R20120723.

[103] The Do Not Track list would allow consumers to opt out of tracking in a similar manner to the "Do Not Call" list for consumers to opt out of telemarketing.

[104] Geoff Duncan, *Why Do Not Track May Not Protect Anybody's Privacy*, DIGITAL TRENDS, (June 9, 2012), http://www.digitaltrends.com/mobile/why-do-not-track-may-not-protect-anybodys-privacy/#ixzz3CMDT9hMu.

[105] *Id.*

> tracked. If the value is a "0," it means the user consents to being tracked. If the header is missing, it means the user isn't supplying any preference at all about tracking.[106]

Debate has continued between advocates for and against a governmental regulated policy, and the Obama administration has urged for industry setting standards before, as a precursor to the necessity of governmental regulation but the Working Group—consisting[107] of industry organizations such as the Direct Advertising Alliance (DAA), Direct Marketing Association (DMA), The Interactive Advertising Bureau (IAB), and The Network Advertising Initiative (NAI)—could not reach a consensus on if and how to orchestrate such a policy:

> To privacy advocates, it is halting data collection so a consumer can surf the Web without any prying eyes collecting information about their online activities for economic gain. To the industry, however, it means not targeting ads to a consumer based on their Web viewing history, but data collection would continue for other purposes.[108]

In a Zogby International online survey of 2,111 U.S. adults, 79% were in support of a national Do Not Track list.[109]

In 2010 the Federal Trade Commission issued a report of its findings, recommending a mandatory Do Not Track option to be available to internet users; however, because the Federal Trade Commission does not have the authority to mandate such a policy, it would have to wait for an act of Congress to be able to enforce such legislation.[110] In 2013, Senate Commerce, Science and Transportation Committee Chairman, Senator Jay

---

[106] Duncan, *supra* note 104, at 21.

[107] Kate Tummarello, *"Do Not Track" Effort in Trouble*, THE HILL, (Sept. 17, 2013), http://thehill.com/policy/technology/322701-do-not-track-group-should-give-up-departing-online-ad-reps-say#ixzz3CMJyFEzq.

[108] Melvin, *supra* note 102, at 20.

[109] *Results from June 4-7 Nationwide Poll*, ZOGBY (June 7, 2010), http//:www.zogby.com.

[110] Gregory Karp, *FTC Proposes 'Do Not Track' List to Protect Internet Users: Privacy Advocates Cheer Recommendation as Good First Step, Industry Officials Say They are Moving That Way Through Self-Regulation*, CHI. TRIB. (Dec. 2, 2010), http://articles.chicagotribune.com/2010-12-02/business/sc-biz-1202-do-not-track-2-20101202_1_behavioral-advertising-information-practices-web-sites.

Rockefeller, proposed the creation of a federal Do Not Track list to be enforced by the Federal Trade Commission,however, to date, no federal legislation has been adopted addressing the issue.[111]
In 2013, California passed its own Do Not Track policy, building upon privacy policy disclosure legislation, to require websites to disclose both how they respond to Do Not Track requests and whether they allow or use third party tracking.[112] The enacted statute, California Business & Professions Code, Section 22575, titled "Commercial Web site operators; posting of privacy policy; violation of subdivision for failure to post policy; policy requirements" provides:

> (a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.
>
> (b) The privacy policy required by subdivision (a) shall do all of the following:
>
> > (1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.
> > (2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or

---

[111] Anne Flaherty, *Senate Chairman Calls for 'Do Not Track' Bill*, PHYS. ORG (Apr. 24, 2013), http://phys.org/news/2013-04-senate-chairman-track-bill.html (last visited Sept. 8, 2014).

[112] CAL. BUS. & PROF. CODE § 22575 (West 2008 & Supp. 2014); *see also* Hadjipetrova & Poteat, *supra* note 4, at 15; Kamala D. Harris, *Making Your Privacy Practices Public*, at 7 (May 2014), http://www.reedsmith.com/files/Uploads/Documents/making_your_privacy_practices_public.pdf.

> online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.
> (3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.
> (4) Identify its effective date.
> (5) Disclose how the operator responds to Web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection.
> (6) Disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service.
> (7) An operator may satisfy the requirement of paragraph (5) by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice.[113]

The California legislature also provided for an enforcement mechanism, California Business & Professions Code, Section 22576, titled "Violation of section for failure to comply with provisions of posted privacy policy,"[114]

V. CONCLUSION

As society's access to technology grows, so does the access to information that individuals might mistakenly assume to be privately protected. Maryland's progressive stance on regulating and enforcing digital privacy protections, coupled with recent consistent legislation reflecting a local importance on increased regulation and the Internet Privacy Unit's ability to effectively prosecute violations of digital privacy in a pivotal role to adopt legislation such as California's Do Not Tr

---

[113] CAL. BUS. & PROF. CODE § 22575 (West 2008 & Supp. 2014) (emphasis added).

[114] CAL. BUS. & PROF. CODE § 22576 (West).